

WHAT IS CLAIMED

1. A method of preventing intrusions on a node of a network, comprising:
  - monitoring, by a first layer of an intrusion prevention system, application data of applications running at on the node;
  - monitoring, by a second layer of the intrusion prevention system, transport layer data of the node; and
  - monitoring, by a third layer of the intrusion prevention system, network layer data of the node.

10

2. The method according to claim 1, wherein monitoring network layer data of the node further comprises monitoring network layer data of the node by the third layer of the intrusion prevention system bound to a media access control driver and a protocol driver of an instance of a network stack of the node.

15

3. The method according to claim 1, wherein monitoring transport layer data of the node further comprises monitoring transport layer data of the node by the second layer of the intrusion prevention system bound to a transport driver interface of an instance of a network stack of the node.

20

4. The method according to claim 1, wherein monitoring application layer data of the node further comprises monitoring application layer data of the node by the first layer of the intrusion prevention system, the first layer interfacing with the second layer by a dynamically linked library.

25

5. The method according to claim 1 further comprises interfacing the first layer of the intrusion prevention system with a file system.

6. The method according to claim 5, wherein interfacing the first layer of the intrusion prevention system with a file system further comprises interfacing the first layer of the intrusion prevention system with a file system comprising at least one of an events-database for archiving intrusion-related events detected by the intrusion

10014006-1  
PATENT APPLICATION

prevention system, a report database for storing reports related to intrusion-related events detected by the intrusion prevention system and a signature file database.

7. The method according to claim 6, further comprising providing, by the  
5 first layer of the intrusion prevention system, one or more signature files maintained  
in the signature file database to the third layer of the intrusion prevention system.

8. The method according to claim 1, further comprising engaging a  
communication session between the first layer of the intrusion prevention system and  
10 a management client of an intrusion prevention system running on a second node of  
the network.

9. A computer-readable medium having stored thereon a set of  
instructions to be executed, the set of instructions, when executed by a processor,  
15 cause the processor to perform a computer method of:

monitoring application layer data, by a first layer of an intrusion prevention  
system comprised of the instructions, of a node of a network, the node comprising the  
processor;

20 monitoring transport layer data, by a second layer of the intrusion prevention  
system, of the node of the network; and

monitoring network layer data, by a third layer of an intrusion prevention  
system, of the node of the network.

10. The computer readable medium according to claim 9, further  
25 comprising a set of instructions that, when executed by a processor, cause the  
processor to perform a computer method of binding the third layer with a media  
access control driver and a protocol driver of an instance of a network stack running  
on the node.

30 11. The computer readable medium according to claim 10, wherein  
binding the third layer with a media access control driver and a protocol driver further

comprises binding the third layer with the media access control driver and the protocol driver upon initialization of the network stack.

12. The computer readable medium according to claim 9, further  
5 comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of binding the second layer with a transport driver interface of an instance of a network stack running on the node.

13. The computer readable medium according to claim 12, wherein  
10 binding the second layer with a transport driver interface further comprises binding  
the second layer with the transport driver interface at initialization of the network  
stack.

14 The computer readable medium according to claim 9, further  
15 comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of communicating, by the first layer, with a file system.

15. The computer readable medium according to claim 9, further  
comprising a set of instructions that, when executed by a processor, cause the  
processor to perform a computer method of communicating, by the first layer, with a  
management application running on a second node of the network

16 The computer readable medium according to claim 14, further  
25 comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of archiving intrusion related events detected by the intrusion protection system in a database of the file system.

17. A node of a network, comprising:

a central processing unit;

a memory module for storing data in machine readable format for retrieval and

5 execution by the central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver, the memory module storing an instance of an intrusion protection system application operable to monitor application layer data and an intrusion prevention system transport service provider layer, and the operating system

10 having an intrusion prevention system network filter service provider bound to the media access control driver and the protocol driver.

18. The node according to claim 17, further comprising a file system, the intrusion protection system application operable to communicate with the file system.

15

19. The node according to claim 18, wherein the file system comprises a database, the intrusion prevention system application operable to log intrusion-related data in the database, the intrusion-related data obtained by at least one of the intrusion prevention system application, the intrusion prevention system transport service provider and the intrusion prevention system network filter service provider.

20

PENTECH INNOVATION INC.